BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin pesat pada zaman sekarang ini membuat kebutuhan manusia akan informasi semakin meningkat. Era digitalisasi telah membawa banyak keuntungan bagi teknologi modern, termasuk peningkatan efisiensi, aksesibilitas, dan inovasi. Kemajuan ini juga memungkinkan setiap orang dengan mudah menggunggah maupun mengunduh berbagai konten yang ada di internet, sehingga pertukaran informasi dapat berlangsung secara cepat.

Di era digital yang semakin terhubung, keamanan data dan informasi menjadi kebutuhan vital para pengguna internet saat ini untuk memastikan privasi mereka tetap terjaga. Kemajuan teknologi informasi dan komunikasi telah memperluas cakupan dan kompleksitas ancaman keamanan siber. Data pribadi, informasi rahasia, dan konten hak cipta menjadi target utama serangan siber yang semakin canggih[1]. Oleh karena itu, perlindungan data dan privasi menjadi sangat mendesak dan memerlukan pendekatan yang inovatif dan efektif.

Salah satu temuan yang mengkhawatirkan seiring dengan penggunaan teknologi *voice assistant* dan sistem pengenalan suara dalam kehidupan sehari-hari adalah *Dolphin Attack*, sebuah penelitian keamanan yang dikembangkan oleh tim peneliti dari Zhejiang University, China, pada tahun 2017 sebagai bukti konsep untuk mengekspos kerentanan sistem pengenalan suara[2]. Penelitian ini mendemonstrasikan bagaimana perintah suara dapat dimodulasi ke frekuensi ultrasonik yang tidak dapat didengar manusia namun masih dapat diinterpretasikan oleh perangkat seperti *smartphone* dan *smart speaker*.

Serangan ini melibatkan modifikasi sinyal audio dengan cara yang hampir tidak terdeteksi oleh telinga manusia [3], tetapi dapat mengelabui sistem pengenalan suara untuk memberikan respon yang diinginkan oleh penyerang. Meskipun masih berstatus penelitian akademis tanpa laporan penggunaan kejahatan nyata secara massal, *Dolphin Attack* menjadi perhatian serius dalam dunia keamanan siber karena mengungkap celah fundamental pada sistem *voice assistant* modern.

Oleh karena itu, dengan meningkatnya jumlah data yang dihasilkan dan dipertukarkan secara digital, teknik keamanan yang kuat dan efektif menjadi sangat diperlukan. Sistem keamanan digital yang telah ada, seperti Kriptografi, *Watermarking*, dan Steganografi, memainkan peran krusial dalam melindungi integritas dan kerahasiaan data digital [4].

Kriptografi adalah ilmu dan teknik yang digunakan untuk melindungi informasi dengan cara mengubahnya menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang [5]. Pada *Watermarking*, informasi identifikasi atau

hak cipta disisipkan ke dalam media digital seperti gambar, audio, atau video [6]. Dengan konsep yang mirip dengan *Watermaking*, Steganografi lebih berfokus pada penyembunyian informasi tanpa terdeteksi dan tidak mempengaruhi kualitas atau tampilannya secara signifikan [7].

Meskipun Kriptografi dan *Watermarking* memiliki kegunaan yang berbeda dalam melindungi data, Steganografi menawarkan keuntungan yang lebih besar dalam menyembunyikan pesan rahasia di dalam media digital, seperti citra atau audio [8], dengan kemampuannya untuk menyembunyikan keberadaan pesan agar tidak terdeteksi oleh orang yang tidak memiliki akses. Kemampuan Steganografi audio menjadi metode yang efektif untuk menyembunyikan pesan rahasia di dalam file audio, seperti file MP3 atau WAV.

Pada steganografi berbasis audio, terdapat beberapa metode yang digunakan untuk menyisipkan pesan rahasia. Metode tersebut diantaranya adalah *Echo Hiding, Least Significant Bit, Phase Coding, Parity Coding* dan *Spread spectrum* [9]. Metode *Spread spectrum* merupakan teknik steganografi di mana informasi rahasia didistribusikan ke seluruh rentang frekuensi dengan menggunakan kode yang tidak berhubungan langsung dengan sinyal audio asli. Metode ini juga menjadi metode steganografi yang paling efektif dan kuat *(robust)* untuk melindungi data [10].

Metode penyisipan pesan rahasia dengan menggunakan teknik *spread spectrum* sudah banyak dilakukan sebelumnya. Pada penelitian [11], teknik *spread spectrum* merupakan teknik yang menyebarkan sinyal melalui *bandwidth* yang lebih lebar daripada *bandwidth* sinyal informasi. Format audio yang digunakan sebagai *cover object* adalah .WAV karena sifatnya yang tidak terkompresi sehingga lebih cocok untuk menyisipkan data tanpa penurunan kualitas yang signifikan. Penelitian ini menyimpulkan teknik *spread spectrum* efektif untuk menyisipkan pesan rahasia ke dalam audio, dimana proses penyisipan dan ekstraksi pesan rahasia melibatkan transformasi *Fast Fourier Transform (FFT)* dan *Pseudo-Noise Random (PRN)* memungkinkan penyebaran pesan yang sulit dideteksi. Namun, peningkatan ukuran pesan rahasia dapat memengaruhi kualitas audio secara objektif, yang ditandai dengan nilai *Peak Signal to Noise Ratio (PSNR)* menurun.

Pada penelitian [12], dibuat rancangan untuk mengimplementasikan salah satu teknik dari *spread spectrum*, yaitu DSSS (*Direct Sequence Spread spectrum*). Penelitian ini menyimpulkan bahwa sistem steganografi audio multikanal berbasis *MPEG Surround* (MPS) menggunakan metode *Direct Sequence Spread spectrum* (DSSS) dapat menyisipkan pesan objek ke dalam sinyal *downmix* sebagai audio *cover*. Audio multikanal menjadi input audio pada encoder *MPEG Surround*. Kemudian sinyal *downmix*, sinyal residual, dan parameter spasial akan diekstraksi dari *encoder* MPS. Pesan rahasia sebagai pesan objek dikalikan dengan kunci *PN Sequence* menggunakan operasi X-OR pada *encoder* DSSS sehingga hasilnya akan menghasilkan data *spread spectrum* yang akan disisipkan ke dalam sinyal audio cover. Sinyal *downmix* sebagai audio *cover* disisipkan dengan pesan objek dalam proses penyisipan dan akan menghasilkan sinyal audio yang memiliki pesan rahasia

yang disebut sinyal stego *downmix*. Pesan objek teks dapat berhasil diekstraksi dengan rata-rata *Bit error rate* (BER) yang kecil.

Pada penelitian ini, secara khusus akan dilakukan analisis terhadap pengaruh level hierarki sistem *downmix MPEG Surround* terhadap kinerja steganografi audio menggunakan metode *Spread spectrum*. Analisis ini dilakukan dengan membandingkan dua skenario penempatan data rahasia, yaitu proses penyisipan sebelum *downmix* dan setelah *downmix*, guna melihat bagaimana distribusi energi pesan memengaruhi kualitas audibilitas dan keberhasilan ekstraksi. Selain itu, penelitian ini ingin melihat apakah terdapat pengaruh yang signifikan jika level hierarki dari struktur pohon *downmix MPEG Surround* dikurangi. Pengurangan kompleksitas hierarki ini dianalisis untuk menentukan titik optimal antara tingkat audibilitas gangguan pada audio (SNR) dan tingkat kesalahan ekstraksi pesan (BER) pada berbagai kondisi sistem, yang sebagaimana menjadi parameter pengukur yang krusial untuk menunjukkan keberhasilan proses Steganografi[13]. Penelitian ini disusun pada Tugas Akhir berjudul "Analisis Pengaruh Sistem Hierarki *Downmixing MPEG Surround* untuk Steganografi Audio menggunakan metode *Spread spectrum.*"

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini yaitu sebagai berikut.

1. Bagaimana pengaruh mekanisme penyisipan pesan yang dilakukan pada hierarki sistem *downmix MPEG Surround* untuk Steganografi audio?
2. Bagaimana pengaruh tingkat hierarki *downmix MPEG Surround* untuk Steganografi audio?

1.3 Tujuan

Tujuan dari penelitian ini adalah:

1. Menganalisis pengaruh mekanisme penyisipan pesan pada setiap tahapan hierarki sistem *downmix MPEG Surround* terhadap performa steganografi audio.
2. Mengevaluasi dampak variasi tingkat hierarki *downmix MPEG Surround* terhadap aspek *imperceptibility* dan ketahanan pesan rahasia yang disisipkan.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Penelitian berfokus pada level hierarki sistem *downmix MPEG Surround* setelah melalui proses penyisipan dengan metode *Spread spectrum*.
2. Aplikasi yang digunakan dalam analisis kinerja hierarki sistem *downmix MPEG Surround* untuk steganografi audio menggunakan teknik *spread spectrum* yaitu MATLAB R2021b.
3. Pesan yang dikirim berupa deretan bit biner acak bernilai 1 dan 0 yang direpresentasikan ke dalam format bipolar menggunakan teknik pengkodean

NRZ (Non-Return-to-Zero).

4. Sampel audio yang digunakan sebanyak 5 buah berformat .WAV, dengan durasi masing-masing audio 12 detik dan laju pengambilan sampel (*sample rate*) sebesar 48 kHz.
5. Metode penyisipan pesan rahasia yang digunakan adalah *Spread spectrum*.
6. Hasil dari penelitian ini menguji nilai BER pesan rahasia dengan panjang *frame* bernilai 1024, 2048, 3072, 4096, dan 5120.
7. SNR audio diuji dengan variasi ukuran *frame* bernilai 1024, 2048, 3072, 4096, dan 5120.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini yaitu memberikan pemahaman tentang bagaimana variasi level hierarki sistem *downmix MPEG Surround* memengaruhi *imperceptibility* audio dan efektivitas penyisipan data menggunakan metode *Spread Spectrum.*

1.6 Sistematika Penulisan

Sistematika penulisan dari tugas akhir ini adalah:

BAB I PENDAHULUAN

Bab ini berisi uraian latar belakang penelitian, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang teori dasar yang mendukung dalam penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang penjelasan dan langkah-langkah mengenai penelitian yang dilakukan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan hasil dan pembahasan mengenai tugas akhir yang telah dilakukan

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapatkan dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.